代数幾何符号のための代数曲線論 (諸分野との協働による数理科学のフロンティア)

AUTHOR(S):

川北, 素子

CITATION:

川北, 素子. 代数幾何符号のための代数曲線論 (諸分野との協働による数理科学のフロンティア). 数理解析研究所講究録 2011, 1752: 3-6

ISSUE DATE:

2011-07

URL:

http://hdl.handle.net/2433/171164

数理解析研究所講究録
第1752巻 2011年 3-6

代数幾何符号のための代数曲線論

滋賀医大・JST さきがけ　川北 素子 (Motoko Kawakita)
Department of Mathematics
Shiga University of Medical Science

§1. 代数幾何符号の発見

1977年に Goppa [5] が代数幾何符号を発見し，純粋数学である代数曲線論が，工学である符号理論に役立つことが判明した．活発に研究された結果，符号化，復号化の多くの課題が解決された [12]．本稿では，代数曲線から構成される代数幾何符号の評価を紹介したのち，有限体上の代数曲線論の近年の発展と現状を概説したい．

まず符号理論の目標を復習しよう．q を素数ベキとし，有限体 $\mathbb{F}_q$ 上で，符号長 n，情報次元 k，最小距離 d の $[n, k, d]$ 線形符号に対し，符号化率 $R := \frac{k}{n}$，相対距離 $\delta := \frac{d}{n}$ と定義する．復号を考慮しない場合，n，R，δ の内二つを固定したとき，残りの一つが大きい方がよい符号である．

一方で有限体 $\mathbb{F}_q$ 上種数 g の代数曲線 C から，下記の条件を満たす q 元線形符号が構成できる:

$$n \leq \#C(\mathbb{F}_q),\ 1 \leq k \leq n,\ n-k+1-g \leq d \leq n-k+1.$$

ここで $\#C(\mathbb{F}_q)$ は代数曲線 C の $\mathbb{F}_q$ 有理点数を表わす．最後の式から

$$R+\delta \geq 1-\frac{g-1}{n}$$

が得られるので，種数 g の代数曲線において，有理点を多数もつものがよい符号を構成することが分かる．

代数曲線論において，

$$N_q(g) := \max\{\#C(\mathbb{F}_q) \mid C : \text{種数 } g \text{ の代数曲線}\}$$

とおき，$\mathbb{F}_q$ 有理点数がこの値に到達する代数曲線を optimal 曲線という．すなわち純粋数学の問題として

「すべての有限体 $\mathbb{F}_q$ と種数 g に対して optimal 曲線を決定せよ．」

を解決することが，論理的に最良の符号を与えることになる．

§2. 代数曲線論の発展

1933 年に Hasse が楕円曲線，1941 年に Weil が一般種数の代数曲線について

$$N_q(g) \leq q + 1 + 2g\sqrt{q}$$

を示した．Hasse–Weil 上界といい，この上界に到達する代数曲線を最大曲線という．代数幾何符号が発見されてから，数学者が再びこの問題に興味をもつこととなった．

1981 年に Ihara [6] が

$$N_q(g) \leq q + 1 + \lfloor (\sqrt{(8q+1)g^2 + 4(q^2-q)g} - g)/2 \rfloor$$

を与え，これは $g > (q - \sqrt{q})/2$ のとき Hasse–Weil 上界より優れている．ここで $\lfloor\ \rfloor$ はガウス記号を表わす．

また 1983 年に Serre [11] が Hasse–Weil 上界を改良し，

$$N_q(g) \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor$$

を与えた．Hasse–Weil–Serre 上界とよぶ．さらに Serre [10] によると，代数曲線が有限体 $\mathbb{F}_q$ 上で，この上界に達するならば，その商曲線もこの上界に達する．

最大曲線について，Garcia, Stichtenoth ら [2] の研究がある．有限体 $\mathbb{F}_{q^2}$ 上の Hermit 曲線

$$y^q + y = x^{q+1}$$

が最大曲線である．多くの最大曲線がこの代数曲線の商曲線として捉えることができる．

2007 年に Giulietti, Korchmáros [4] が初めて Hermit 曲線の商曲線ではない最大曲線を構成した．有限体 $\mathbb{F}_{q^6}$ 上

$$x^q + x = y^{q+1}, \quad y\frac{x^{q^2} - x}{x^q + x} = z^{\frac{q^3+1}{q+1}}$$

で定義された代数曲線である．さらに Fanali, Giulietti [1] は，その商曲線を構成することで多くの最大曲線ができることを示した．

2010 年に Garcia, Stichtenoth ら [3] は，これを一般化した最大曲線を構成した．$n > 0$ を奇数とし，有限体 $\mathbb{F}_{q^{2n}}$ 上

$$x^q + x = y^{q+1}, \quad y^{q^2} - y = z^{\frac{q^n+1}{q+1}}$$

で定義された代数曲線である．Hermit 曲線の商曲線であるかどうか，現在研究が進められている．

最大曲線以外の optimal 曲線について系統的な研究ができていない．van der Geer らによる $N_q(g)$ のデータベースが http://www.manypoints.org/ で公開されているが，種数 4 以上では $N_q(g)$ がほとんど決定されていないことがわかる．このデータベースには，有限体上において多数の有理点をもつ代数曲線の結果も集められており，代数幾何符号のための代数曲線論の進展を知る上で役に立つ．

§3. Hasse–Weil–Serre 上界に達する代数曲線

最後に筆者 の研究を少し紹介する．以下 p を素数とする．

定理. [7] 有限体 $\mathbb{F}_p$ 上で代数曲線 $D:\ y^{12}=x^4(1-x)$ が Hasse–Weil–Serre 上界に達する必要十分条件は，$p\equiv 1 \bmod 12$，$\lfloor 2\sqrt{p}\rfloor \equiv 1 \bmod 3$，整数 n が存在して $p=\lfloor\sqrt{p}\rfloor^2+27n^2$ となることである．

定理. [8] 有限体 $\mathbb{F}_p$ 上で代数曲線 $F:\ x^6+y^6=1$ が Hasse–Weil–Serre 上界に達する必要十分条件は，$p\equiv 1 \bmod 12$，$\lfloor 2\sqrt{p}\rfloor \equiv 1 \bmod 3$，整数 n が存在して $p=\lfloor\sqrt{p}\rfloor^2+27n^2$ となることである．

Buniakowski 予想. a，b，c が整数，$a>0$，$\gcd(a,b,c)=1$，$a+b$ と c の少なくとも一方が奇数，さらに b^2-4ac が平方でないとすると，an^2+bn+c の形の素数が無限個存在する．

命題. [7] [8] Buniakowski 予想が正しいとすると，定理の条件を満たす素数が無限個存在する．

命題. [8][9] 楕円曲線を $E_1:y^2=x^3+1$，$E_2:y^2=x^3-1$，$E_3:y^2=x^3+4$，$E_4:y^2=x^3-4$，$E_5:y^2=x^3+\frac{1}{4}$，$E_6:y^2=x^3-\frac{1}{4}$ とおくと，

(i) 代数曲線 D の Jacobian は $J_D\sim E_3\times E_5^2\times E_6$ と完全分解される;

(ii) 代数曲線 F の Jacobian は $J_F\sim E_1^4\times E_2^2\times E_3^2\times E_4\times E_5$ と完全分解される．

これらの楕円曲線の虚数乗法は $\mathbb{Z}[\omega]$ である．

§4. 結び

代数幾何符号が発見されてから，有限体上の代数曲線論の研究が盛んになった．ところが，工学の観点から提起された問題は，純粋数学においても実に難しく，数学者のチャレンジ精神を刺激している．前節の定理は，コンピュータ探索で得られた結果を定式化したものである．この分野では工学，数学，コンピュータサイエンスが交差していて，興味深いことである．

謝辞．本研究は，JST 戦略的創造研究推進事業さきがけの一環として行われたものである．織田孝幸教授，三浦晋示博士との討論に感謝する．

参考文献

[1] S. Fanali, M. Giulietti, Quotient curves of the GK curve, arXiv:0909.2582v1.

[2] A. Garcia, H. Stichtenoth, C. P. Xing, On subfields of the Hermitian function field, Comp. Math. **120**(2000), 137–170.

[3] A. Garcia, G, Güneri, H. Stichtenoth, A generalization of the Giulietti-Korchmaros maximal curve, Adv. Geom. **10**(3)(2010), 427–434.

[4] M. Giulietti, G. Korchmáros, A new family of maximal curves over a finite field, Math. Ann. **343**(2009), 229–245.

[5] V. D. Goppa, Codes on algebraic curves (Russian), Dokl. Akad. Nauk SSSR **259**(6)(1981), 1289–1290.

[6] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, J. Fac. Sci. Tokyo **28**(1981), 721–724.

[7] M. Q. Kawakita, A quotient curve of the Fermat curve of degree twelve attaining the Serre bound, J. Algebra Appl. **4**(2)(2005), 173–178.

[8] M. Q. Kawakita, On quotient curves of the Fermat curve of degree twelve attaining the Serre bound, Internat. J. Math. **20**(5)(2009), 529–539.

[9] M. Q. Kawakita, Complex multiplications of non-maximal curves attaining the Serre bound, Submitted to Natur. Sci. Rep. Ochanomizu Univ.

[10] K. Lachaud, Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis, C. R. Acad. Sci. Paris, Sér. I Math. **305**(16)(1987), 729–732.

[11] J.-P. Serre, Sur le nombre des points rationnels d' une courbe algébrique sur un corps fini, C. R. Acad. Sci. Paris Sér. I Math. **296**(9)(1983) 397–402. (=OEuvres III, No. 128, 658–663.)

[12] H. Stichtenoth, Algebraic Function Fields and Codes, GTM **254**(2008), Springer.